APPARATUS AND METHOD FOR CALCU-LATINGTKIP SBOX VALUE

Abstract

An input port for receiving the 16-bit index value is connected to a plurality of combinatorial logic. The plurality of combinatorial logic directly calculates the TKIP Sbox value based on the index and outputs the TKIP Sbox value on an output port. The plurality of combinatorial logic has a first plurality of combinatorial logic connected to a low part of the index value for calculating a TKIP Sbox left value and a second plurality of combinatorial logic connected to a high part of the index value for calculating a TKIP Sbox right value. The TKIP Sbox value is formed by XORing the TKIP Sbox left value and the TKIP Sbox right value.